



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,026	10/10/2000	Marco Martins	YOR9-2000-0165	2558

48150 7590 08/10/2005

MCGINN & GIBB, PLLC
8321 OLD COURTHOUSE ROAD
SUITE 200
VIENNA, VA 22182-3817

EXAMINER

HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/685,026

Applicant(s)

MARTINS ET AL.

Examiner

Brandon S. Hoffman

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 and 3-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 and 3-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1 and 3-27 are pending in this office action, claim 2 is canceled.
2. Applicant's arguments, filed June 9, 2005, have been considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 24, 25, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Urata (U.S. Patent No. 6,799,272) in view of Kawan (U.S. Patent No. 6,289,324).

Regarding claim 24, Urata teaches a method of preventing counterfeiting of a smart card, comprising:

- Providing a smart card such that none of confidential information and a cryptographic key for authorizing the smart card, is carried on the smart card (col. 2, lines 32-52);

Art Unit: 2136

- Reading said card by a reader such that in each reading, said reader reads only a predetermined small amount of information which makes the card unique (col. 2, lines 32-52).

Urata does not specifically teach a reader for the smart card, but an authentication center that receives the data over a communication system.

Kawan teaches a reader for the smart card (fig. 2, ref. num 210).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a smart card reader, as taught by Kawan, with the method of Urata. It would have been obvious for such modifications because a smart card reader provides the interfacing means for accessing the information on the smart card.

Regarding claim 25, the combination of Urata as modified by Kawan teaches wherein an entire process of said method is performable off-line (see col. 5, lines 47–59 of Kawan).

Regarding claim 27, Urata teaches a method/computer readable medium for preventing counterfeiting and cloning of smart cards, comprising:

Art Unit: 2136

- Providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings (col. 2, lines 32-52).

Urata does not teach wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof.

Kawan teaches wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof (col. 9, lines 36-43).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof, as taught by Kawan, with the method of Urata. It would have been obvious for such modifications because keeping the cryptographic structure secret to only those who emit the card prevents someone from counterfeiting a smart card (see col. 9, lines 36-40 of Kawan).

Claims 1, 3-7, 9-14, 23, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Urata (USPN '272) in view of Kawan (USPN '324), and further in view of Perlman et al. (U.S. Patent No. 5,261,002).

Regarding claim 1, Urata teaches a method/computer readable medium for preventing counterfeiting and cloning of smart cards, comprising:

- Providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings (col. 2, lines 32-52).

Urata does not teach wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof or providing a reader for reading said smart card.

Kawan teaches wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof (col. 9, lines 36-43), and providing a reader for reading said smart card (fig. 2, ref. num 210).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof, as taught by Kawan, with the method of Urata. It would have been obvious for such modifications because keeping the cryptographic structure secret to only those who emit the card prevents someone from counterfeiting a smart card (see col. 9, lines 36-40 of Kawan).

The combination of Urata as modified by Kawan still does not teach including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network.

Perlman et al. teaches including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network (col. 3, lines 38-40, col. 6, lines 37-39, and fig. 1, ref. num 24-30).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a reader including a database of unauthorized smart cards, said reader being online and connected to a network only when said reader is being updated, as taught by Perlman et al., with the system of Urata/Kawan. It would have been obvious for such modifications because the off-line version of the blacklist provides a listing of all users who are intruders; the periodic updating allows a newer list of intruders to be known.

Regarding claim 3, the combination of Urata as modified by Kawan/Perlman et al. teaches wherein an entire process of said method is performable off-line (see col. 5, lines 47-59 of Kawan).

Art Unit: 2136

Regarding claim 4, the combination of Urata as modified by Kawan/Perlman et al. teaches wherein said smart card carries thereon predetermined N channels as C1, C2, ..., CN, where N is an integer, wherein each channel C_i, with i equal to 1, 2, ..., N, carries a pair of numbers (h_i, l_i), and wherein h_i is the ith high number and l_i is the ith low number (see col. 2, lines 32-52 and fig. 1, ref. num 106, 128, and 142 of Urata).

Regarding claim 5, the combination of Urata as modified by Kawan/Perlman et al. teaches further comprising using public key cryptography with associated encoding and decoding functions V_i and V_i⁻¹ in each channel i, wherein each function V_i⁻¹ is known publicly, and V_i is known only to a predetermined party representing an owner of the smart card (see page 6, lines 1-5 of applicants disclosure, applicant submits this information is well known as taught by Menezes et al.).

Regarding claim 6, the combination of Urata as modified by Kawan/Perlman et al. teaches wherein for each i in 1, 2, ..., N, the pair (h_i, l_i) is such that h_i = V_i(l_i), or h_i = V_i(K(l_i)), where K represents a publicly-known cryptographic hash function, and wherein each l_i contains a plurality of symbols for redundancy (see page 6, lines 6-8 of applicants disclosure, applicant submits this information is well known as taught by Menezes et al.).

Regarding claim 7, the combination of Urata as modified by Kawan/Perlman et al. teaches further comprising processing, using an invertible function f which is made

public, such that the low numbers in said smart card satisfy $l(i+j) = f^j(l_i)$, where f^j represents the j^{th} iteration of the function f (see col. 5, line 48 through col. 6, line 25 of Urata).

Regarding claim 9, the combination of Urata as modified by Kawan/Perlman et al. teaches wherein a reader obtains a content of only two of said channels (see col. 2, lines 37-47 of Urata).

Regarding claim 10, the combination of Urata as modified by Kawan/Perlman et al. teaches further comprising periodically communicating, by a reader of said smart card, with a database where a predetermined characteristic of the card is checked (see col. 3, lines 38-40 and fig. 1, ref. num 16-18 of Perlman et al.).

Regarding claim 11, the combination of Urata as modified by Kawan/Perlman et al. teaches wherein the predetermined characteristic comprises whether a smart card has delivered more than a predetermined amount of money to a user of the smart card (see col. 7, lines 21-23 of Perlman et al.).

Regarding claim 12, the combination of Urata as modified by Kawan/Perlman et al. teaches wherein if a card is detected as delivering too much money, the database communicates a corresponding number l_1 to all readers in a network, so that smart

Art Unit: 2136

cards carrying said corresponding number are declined (see col. 7, lines 14-26 of Perlman et al.).

Regarding claim 13, the combination of Urata as modified by Kawan/Perlman et al. teaches wherein said cryptographic structure is changed periodically (see col. 6, lines 33-42 of Urata).

Regarding claim 14, the combination of Urata as modified by Kawan/Perlman et al. teaches wherein said smartcard is invalidated after a predetermined time of usage (see fig. 2, ref. num 42 of Perlman et al.).

Regarding claim 23, the combination of Urata as modified by Kawan/Perlman et al. teaches further comprising performing a final validation of the smart card by at least one of:

- Contacting a central database if an entire transaction is made on-line with no penalty (see col. 6, lines 37-39 of Perlman et al.); and
Checking with a local database in a reader, said local database being refreshed periodically by contact between said local database and said central database (see col. 3, lines 38-40 and fig. 1, ref. num 24-30 of Perlman et al.).

Regarding claim 26, Urata teaches a system for preventing cloning of a smart card, comprising:

Art Unit: 2136

- A smart card such that a cryptographic structure for authorizing the smart card is not carried on the smart card (col. 2, lines 32-52).

Urata does not teach a reader for reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards, wherein said cryptographic structure is kept secret by whoever emits the card or an agent thereof,

Kawan teaches wherein said cryptographic structure is kept secret by whoever emits the card or an agent thereof (col. 9, lines 36-43).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof, as taught by Kawan, with the system of Urata. It would have been obvious for such modifications because keeping the cryptographic structure secret to only those who emit the card prevents someone from counterfeiting a smart card (see col. 9, lines 36-40 of Kawan).

The combination of Urata as modified by Kawan still does not teach a reader for reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards.

Perlman et al. teaches a reader for reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards (col. 3, lines 38-40, col. 6, lines 37-39, and fig. 1, ref. num 24-30).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a reader for reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards, as taught by Perlman et al., with the system of Urata/Kawan. It would have been obvious for such modifications because the off-line version of the blacklist provides a listing of all users who are intruders; the periodic updating allows a newer list of intruders to be known.

Claims 8 and 15-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Urata (USPN '272) in view of Kawan (USPN '324) and Perlman et al. (USPN '002), and further in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, pps. 466-474 (hereinafter Schneier).

Regarding claim 8, the combination of Urata as modified by Kawan/Perlman et al. teaches all the limitations of claims 1, 4, 5, and 6, above. However, the combination of Urata as modified by Kawan/Perlman et al. does not teach wherein a reader includes a random number generator, which, when a card is read, chooses a pair (a, b) of

Art Unit: 2136

distinct numbers with $a < b$ between 1 and N , wherein before processing the smart card, the reader obtains the pair (h_a, l_a) and h_b , and using the public keys V_a^{-1} and V_b^{-1} , checking by the reader whether the pairs (h_a, l_a) and (h_b, l_b) are compatible, and, consequently, that the numbers h_a , l_a , and h_b belong to a same legitimate card.

Schneier teaches:

- Wherein a reader includes a random number generator, which, when a card is read, chooses a pair (a, b) of distinct numbers with $a < b$ between 1 and N , wherein before processing the smart card, the reader obtains the pair (h_a, l_a) and h_b (a step of an RSA algorithm, choose two prime numbers, page 467);
- Using the public keys V_a^{-1} and V_b^{-1} , checking by the reader whether the pairs (h_a, l_a) and (h_b, l_b) are compatible, and, consequently, that the numbers h_a , l_a , and h_b belong to a same legitimate card (a step of an RSA algorithm, page 467).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a random number in the reader, choose a pair of distinct numbers, and using the public keys to check the compatibility of the smart card, as taught by Schneier, with the method of Urata/Kawan/Perlman et al. It would have been obvious for such modifications because these limitations verify a proper smart card based on the key checking, known as a digital signature.

Art Unit: 2136

Regarding claim 15, the combination of Urata as modified by Kawan/Perlman et al./Schneier teaches wherein said pairs (hi, li) to be contained on the smart card are generated by:

- Choosing a prefix of I1 once for all transactions, or changed whenever needed, wherein said prefix is publicly known (a step of an RSA algorithm, see page 467 of Schneier); and
- Providing a sequence, such that the sequence is generated so that a same number is not chosen twice, and so that corresponding other li's are not chosen as new I1s (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 16, the combination of Urata as modified by Kawan/Perlman et al./Schneier teaches further comprising:

- Concatenating the prefix and the sequence to form I1 (a step of an RSA algorithm, forming the product of two primes, see page 467 of Schneier); and
- Choosing a function f which is invertible and is publicly known, to construct I2 = f(I1), I3 f(I2), and so forth (a step of an RSA algorithm, use Euclidean algorithm on two primes, see page 467 of Schneier).

Regarding claim 17, the combination of Urata as modified by Kawan/Perlman et al./Schneier teaches wherein the function f is chosen to be the identity map, in which case I1 = I2 = I3 = ... =IN (a step of an RSA algorithm, where the message is encrypted

Art Unit: 2136

in blocks, where the same encryption method is used for each block, see page 467 of Schneier).

Regarding claim 18, the combination of Urata as modified by Kawan/Perlman et al./Schneier teaches choosing, for a number N , N public key-private key pairs, such that a first private key $V1$ is for computing $h1 = V1(I1)$, a second private key $V2$ is for computing $h2 = V2(I2)$, and so on (a step of an RSA algorithm, where the message is encrypted in blocks, see page 467 of Schneier).

Regarding claim 19, the combination of Urata as modified by Kawan/Perlman et al./Schneier teaches further comprising:

- Verifying whether the smart card is authentic (digital signature of an RSA algorithm, see page 473 of Schneier); and
- Checking whether the smart card is not in a list of cards to be refused (see col. 6, lines 37-39 of Perlman et al.).

Regarding claim 20, the combination of Urata as modified by Kawan/Perlman et al. teaches all the limitations of claim 1, above. However, the combination of Urata as modified by Kawan/Perlman et al. does not teach wherein, when the smart card is read by a reader, a random generator is prompted which provides two integer numbers, a and b , which are not between 1 and N , with $a < b$.

Schneier teaches wherein, when the smart card is read by a reader, a random generator is prompted which provides two integer numbers, a and b, which are not between 1 and N, with $a < b$ (a step of an RSA algorithm, see page 467).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a random number when the smart card is read, the random numbers are a and b, with $a < b$, as taught by Schneier, with the method of Urata/Kawan/Perlman et al. It would have been obvious for such modifications because these limitations select a public key of the reader for use in a public key algorithm. The public key can then be used to encrypt data so that only the intended recipient can decrypt the data.

Regarding claim 21, the combination of Urata as modified by Kawan/Perlman et al./Schneier teaches wherein said numbers a, b are transmitted to the smart card which delivers two high numbers h_a , h_b , and a low number l_a in a channel a, and wherein the pair (a, b), together with a function f in a memory in the reader, are used to compute the low number $l_b = f^{(b-a)}(l_a)$, said memory in said reader delivering public keys V_a^{-1} and V_b^{-1} (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 22, the combination of Urata as modified by Kawan/Perlman et al./Schneier teaches wherein the public keys are used by a comparator together with the pairs (h_a, l_a) and (h_b, l_b) , to verify that the pairs are compatible with the

Art Unit: 2136

corresponding keys, and that the pairs are from a same legitimate card (a step of an RSA algorithm, see page 467 of Schneier).

Response to Arguments

5. Applicant argues that the combination of references would not have arrived at the claimed invention and that Perlman et al. does not teach or disclose "providing a smart card" and "providing a reader for reading said smart card and including a database holding information related to unauthorized smart cards." (See page 16, third full paragraph, page 17, first paragraph, and page 18, first full paragraph).

Regarding applicant's argument, examiner disagrees with applicant. Examiner wants to point out that Kawan was cited as disclosing a smart card reader (fig. 2, ref. num 210), not Perlman et al. The non-final office action (and the current rejection) points out the fact that Kawan discloses the smart card reader. Perlman et al. was added for further showing the feature of blacklists and periodic updates. Applicant has amended independent claim 1 to incorporate the limitations of a database holding information related to unauthorized smart cards.

Prior to this amendment, the claim simply stated "providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings" and "said cryptographic structure can be built only by whoever emits the card or an agent thereof."

The first limitation was clearly taught by Urata to contain a *smart card* that contains a cryptographic structure for authorizing wherein the structure cannot be accessed completely by a small number of readings (see col. 2, lines 32-52 of Urata). This passage shows a key code index being contained in the *smart card*. This key code index cannot be completely accessed by a small number of readings and clearly does not contain any confidential information, as recited in other embodiments of the independent claims. Figure 1 of Urata shows the key code index with its many entries.

The second limitation was clearly taught by Kawan to disclose the cryptographic structure can be built only by whoever emits the card or an agent thereof (see col. 9, lines 36-43 of Kawan). The passage clearly states that *smart cards* can be impervious to counterfeiting as long as the keys (or cryptographic structure) are known only to the issuer of the smart card and the entity supporting the ATM and merchant terminal system. This passage gives way to a motivation to make sure that no one, except for the agent of the card, may build the cryptographic structure – whether it be a set of keys as proposed in Kawan, or a key code index as proposed by Urata.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this office action. Accordingly, **THIS ACTION IS MADE FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within

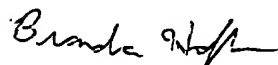
Art Unit: 2136

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

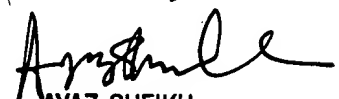
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



BH


AYAZ SHEIKH

SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100